# Data Security, Data Breaches and Security Alerts

*Data security controls are crucial to ensure that customer and company information is protected*

Berthing, Hans Henrik

*Publication date:*
2012

*Document Version*
Early version, also known as pre-print

6th Annual European GRC Summit

Governance, Risk Management and Compliance

6 - 7. June 2012, Radisson Blu Scandinavia Hotel, Copenhagen - Denmark

# Data Security, Data Breaches and Security Alerts Data security controls are crucial to ensure that customer and company information is protected.

*Statsautoriseret revisor og senior advisor Hans Henrik Berthing*

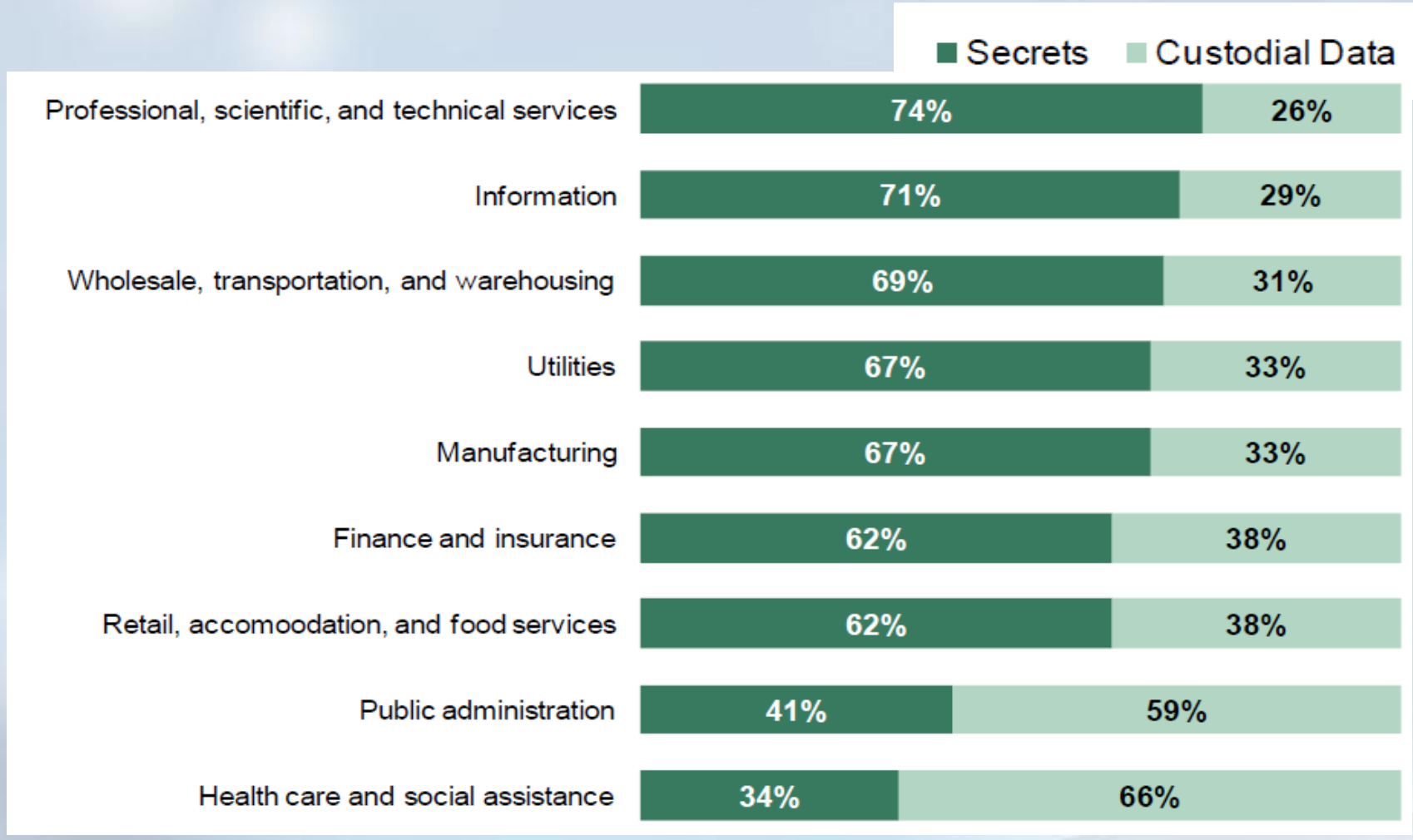
# Agenda

- How to safeguard against the risks associated with groups that are either employed, associated or business partners that have access to data and systems.
- A review of updated controls, user access, separation of system infrastructure, limits and restrictions and proactive system monitoring
- How to monitor periodic risk assessments of information security programs

# About me

- 44 years, married with Louise and dad for Dagmar and Johannes
- CPA, CRISC, CGEIT, CISA and CIA
- ISO 9000 Lead Auditor
- Service Audit Reports (ISAE 3402)
- Extensive experience with Financial Audit, Internal Audit, Internal Controls, SOX, IT Governance, IT Security and IT Assurance
- Instructor, facilitator and speaker
- Senior Researcher & Associated Professor Aalborg University
- Member of IT Advisory Board FSR-danske revisorer

# Company Value




Source :Forrester Consulting for RSA og Microsoft November 2009

# Data Breaches - 2011

- Sony PlayStation
  - Criminal hacker(s) obtained names, addresses, email addresses, dates of birth, PSN/Qriocity password and login, and online IDs for multiple users.
  - Hackers gained access to 101.6 million records, including 12 million unencrypted credit card numbers
- Epsilon, an email service provider for companies
  - 75 client companies.  Email addresses and customer names
  - Millions of customers received notices from a growing list of companies, **making this the largest security breach ever**.
  - Conservative estimates: 50 to 60 million customer email addresses. May have reached 250 million.

Source: Privacy Rights Clearinghouse, December 16, 2011

# Data Breaches - today

- LinkedIn investigates hacking claims
  - Business social network examines claims by security analysts that more than 6 million users' details have been posted online
  - Change your password in next break!!!!
- TV2 leaks Danish Football Players identity
  - Nicklas Bendtner & Dennis Rommedahls passport were shown in TV so the players social security numbers could be read
  - Players get help from policemen
- Kindergarten lacks privacy data

Source: Guardian June 6, 2012 & TV2 June 5, 2012

# Data Breaches

- Verizon's 2012 Data Breach Investigations Report suggests that 97% of the breaches they investigated could have been prevented had the victimized business implemented rudimentary security controls like antimalware tools and effective patch management processes.
- Other sources of security incident data shows that the vast majority of breaches would be defeated if organizations would take simple steps to protect themselves.

Source: Verizon 2012 Data Breach Investigations Report

# Lessons learned

- Importance of password hygiene. Passwords are frequently the only thing protecting our private information from prying eyes.
- Websites with personal information require just a user name and password for protection.
- Password-protected web sites are becoming more vulnerable because often people use the same passwords on numerous sites.
- Sophos: More than 30% of users recycle the same password for every site that they access.
- Spear-phishing: "Hello Mr. Berthing, Because of the recent hacking incident affecting some Acme customers, we are asking you to visit this website [URL provided] and update your security settings."
- Epsilon breach: Highlights the risk of cloud-based computing systems and the need for greater cloud security measures.

Source: Privacy Rights Clearinghouse, December 16, 2011

# SANS: 20 Critical Controls

Controls grouped into specific categories

- *Quick wins.*
- *Improved visibility and attribution*
- *Hardened configuration and improved information security hygiene.*
- *Advanced.*

Source: SANS Institute ***Version 3.1 October 3, 2011***

# SANS: 20 Critical Controls

- First-hand knowledge and input on how attacks are carried out and the defensive techniques that are most important to thwart provided by a wide range of people and organizations
- More than 100 other collaborators
- Most prevalent and damaging attack types and scenarios so appropriate defenses could be identified.
- Includes controls that can be continuously monitored and validated at least in part in an automated manner and some that must be validated manually.
- Control categories are prioritized based on the NSA attack mitigation scores.
- The process of gathering the controls and subcontrols focused on identifying the highest priority defenses and represents a subset of controls found in other audit guidelines and documents.
- The control areas is important and offers high-priority techniques for thwarting real-world attacks.

Source: SANS Institute ***Version 3.1 October 3, 2011***

# SANS: 20 Critical Controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware
6. Application Software Security
7. Wireless Device Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Source: SANS Institute ***Version 3.1 October 3, 2011***

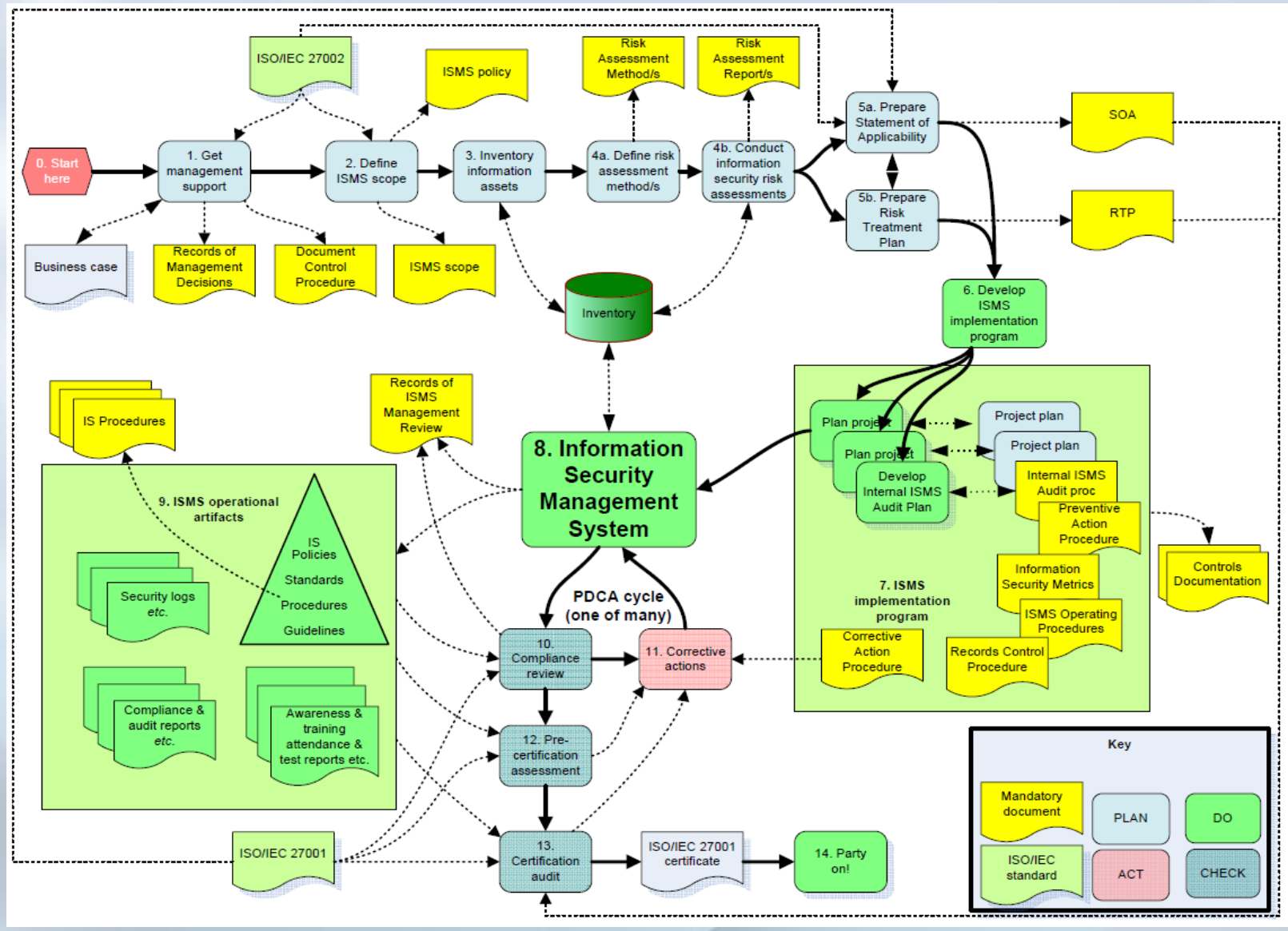
# SANS: 20 Critical Controls

11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Loss Prevention
18. Incident Response Capability
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

Source: SANS Institute ***Version 3.1 October 3, 2011***

# ISO/IEC27001

# PDCA ISO 27001



# Risk IT Includes

***The Risk IT Framework***

- Summary + Core Framework
- Helps convey the risk landscape and processes and prioritise activities
- Available as a free download to all

***The Risk IT Practitioner Guide***

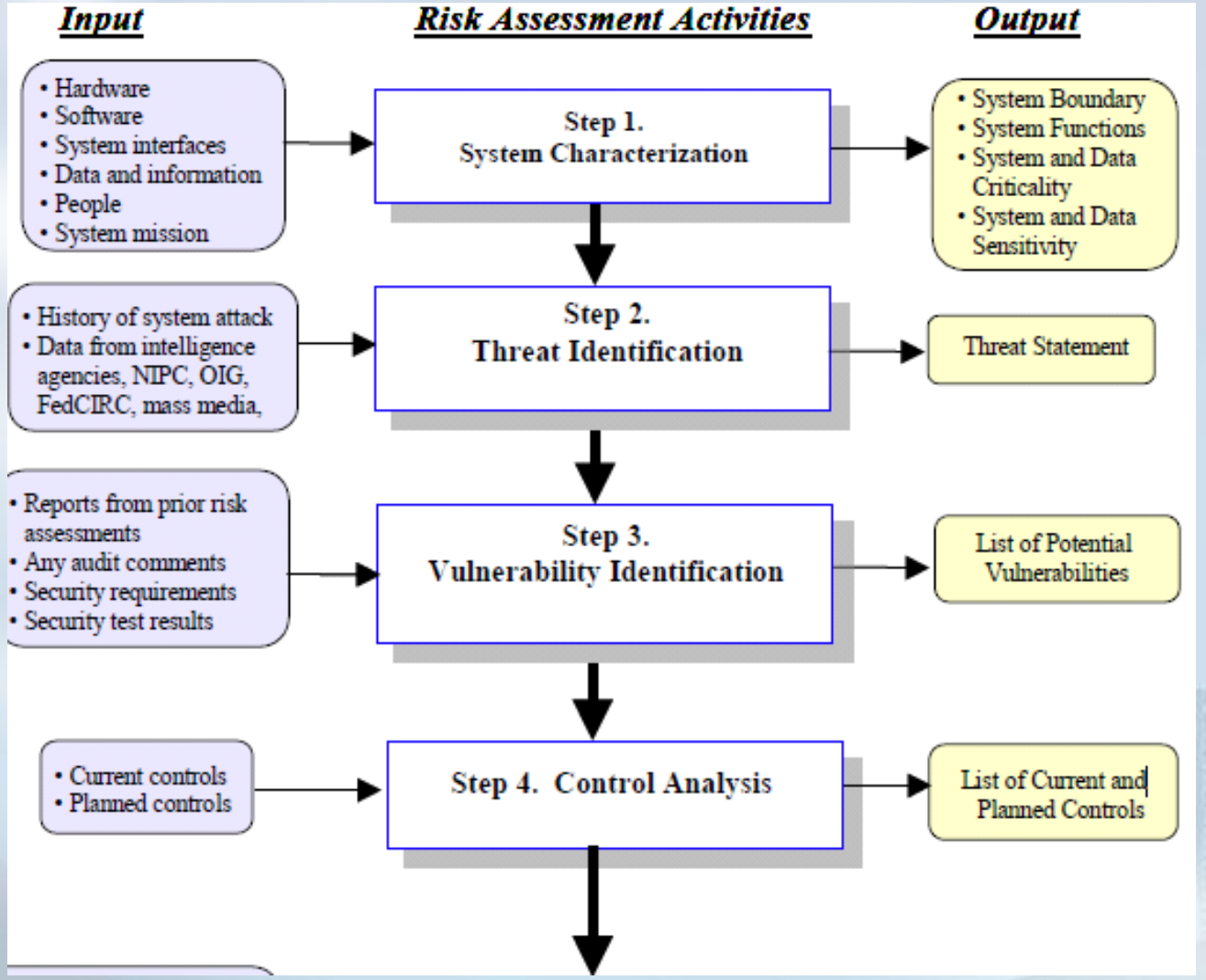
- Provides *practical* guidance on improving risk management activities
- Available as a free download for ISACA members only

(Both publications are available for purchase in print version)

***www.isaca.org/riskit***

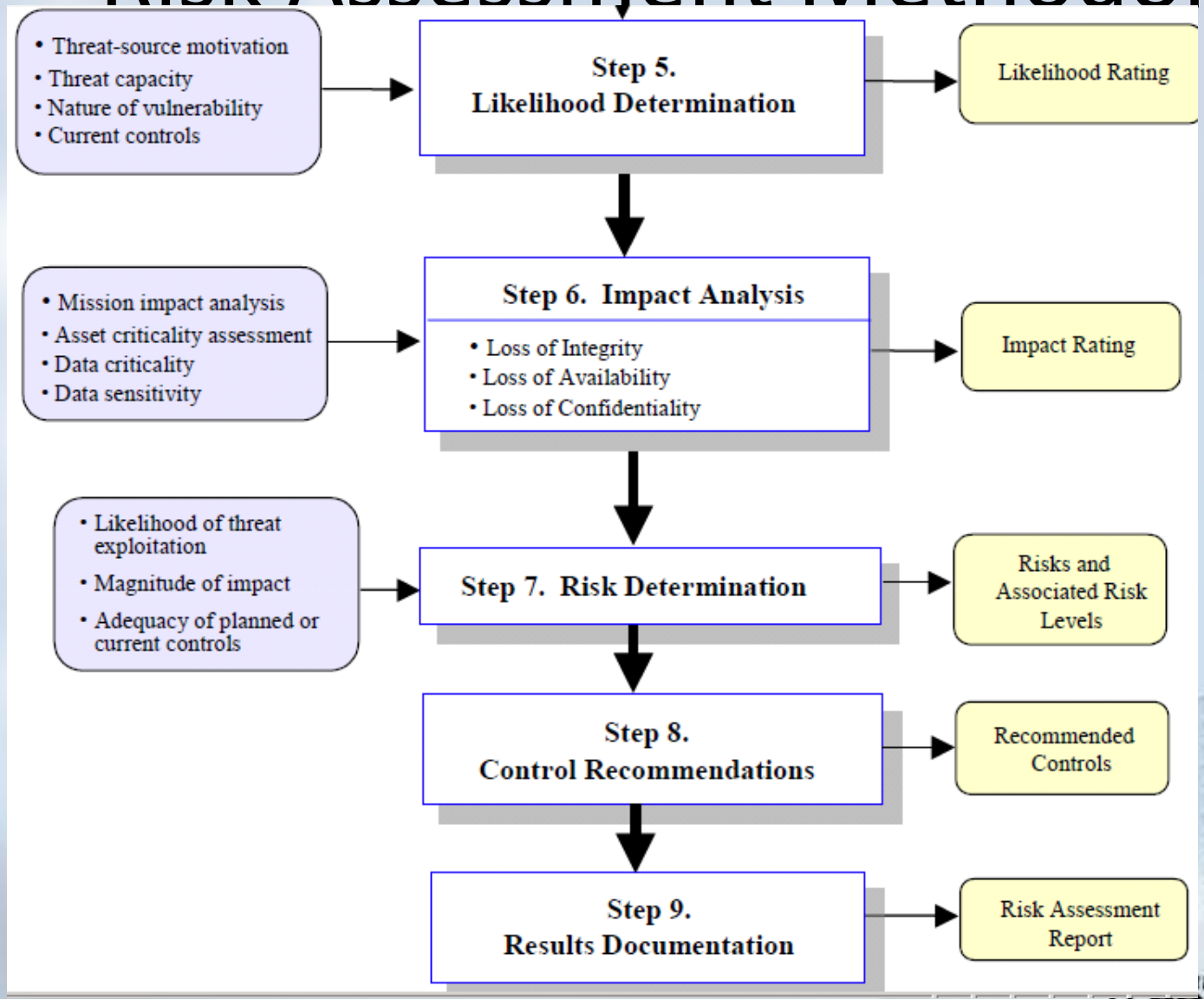
Source: Risk IT, ISACA

# Risk Assessment Methodology




Source: NIST: **Risk Management Guide for Information Technology Systems**

# Risk Assessment Methodology




Source: NIST: **Risk Management Guide for Information Technology Systems**

# System-Related Information

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity

Source: NIST: **Risk Management Guide for Information Technology Systems**

# Risk-Level Matrix

| Threat Likelihood | Impact | | |
|---|---|---|---|
| | | | ***High*** (100) |
| ***High*** (1.0) | **Low** 10 X 1.0 = 10 | **Medium** 50 X 1.0 = 50 | **High** 100 X 1.0 = 100 |
| ***Medium*** (0.5) | **Low** 10 X 0.5 = 5 | **Medium** 50 X 0.5 = 25 | **Medium** 100 X 0.5 = 50 |
| ***Low*** (0.1) | **Low** 10 X 0.1 = 1 | **Low** 50 X 0.1 = 5 | **Low** 100 X 0.1 = 10 |

*Risk Scale: High ( >50 to 100); Medium ( >10 to 50); Low (1 to 10)*[8]

Source: NIST: **Risk Management Guide for Information Technology Systems**

# Risk Scale and Necessary Actions

| | Risk Description and Necessary Actions |
|---|---|
| **High** | If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. |
| **Medium** | If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. |
| **Low** | If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk. |

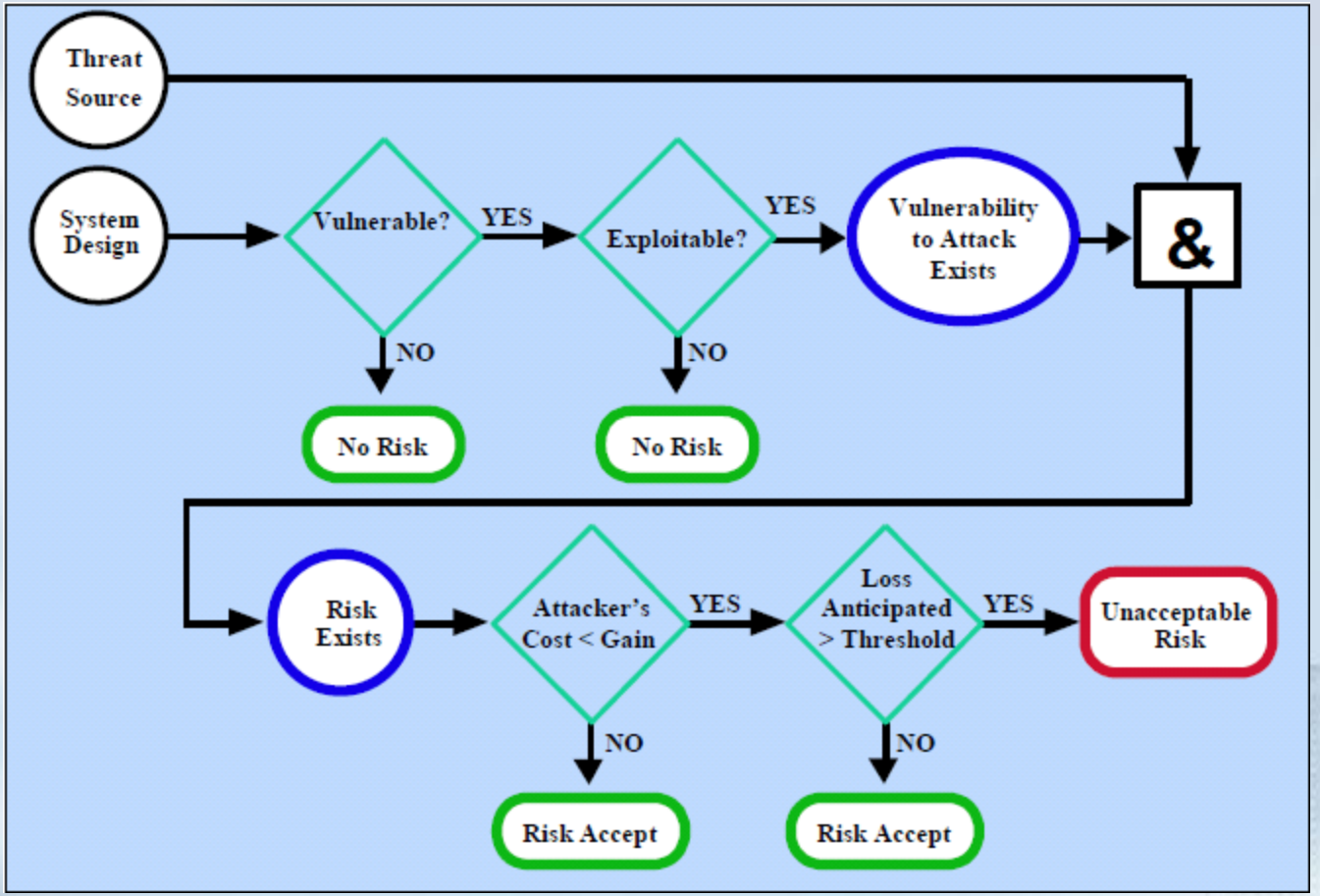
Source: NIST: **Risk Management Guide for Information Technology Systems**

# Control Recommendations

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

Source: NIST: **Risk Management Guide for Information Technology Systems**

# Risk Mitigation Action Points




Source: NIST: **Risk Management Guide for Information Technology Systems**

# Good security practise

- The risk assessment process is usually repeated at least every 3 years for federal agencies
- Risk management should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization's business objectives or mission.
- Specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies

Source: NIST: **Risk Management Guide for Information Technology Systems**

# Key for success

Successful risk management program will rely on

1. senior management's commitment;
2. the full support and participation of the IT team
3. the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization;
4. the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and
5. ongoing evaluation and assessment of the IT-related mission risks.

Source: NIST: **Risk Management Guide for Information Technology Systems**

6th Annual European GRC Summit

Governance, Risk Management and Compliance

6 - 7. June 2012, Radisson Blu Scandinavia Hotel, Copenhagen - Denmark

- Thank You


- Hans Henrik Berthing,
- CPA, CRISC, CGEIT, CISA CIA
- Phone: +45 35 36 33 56
- Mobile: +45 22 20 28 21
- Mail: hhberthing@verifica.dk

# Sony PlayStation – 2011

- External intrusion on PlayStation Network (PSN) and its Qriocity music service around April 19.
- Sony blocked users from playing online games or accessing services like Netflix and Hulu Plus on April 22.
- The blockage lasted for seven days.
- Sony believes criminal hacker(s) obtained names, addresses, email addresses, dates of birth, PSN/Qriocity password and login, and online IDs for multiple users.
- The attacker may have also stolen users' purchase history, billing address, and password security questions.
- Over the course of the next several months, Sony discovered that the hackers gained access to 101.6 million records, including 12 million unencrypted credit card numbers

Source: Privacy Rights Clearinghouse, December 16, 2011

# Sony PlayStation – 2011

- The Sony breach highlights the importance of password hygiene.
- Passwords are frequently the only thing protecting our private information from prying eyes.
- Many websites that store your personal information (for example web mail, photo or document storage sites, and money management sites) require just a user name and password for protection.
- Password-protected web sites are becoming more vulnerable because often people use the same passwords on numerous sites.
- One study by Sophos, a security firm, found that more than 30% of users recycle the same password for every site that they access. In this case, the stolen passwords were unencrypted, meaning the criminal could potentially "break in" to other sites if the victims used the same password more than once

Source: Privacy Rights Clearinghouse, December 16, 2011

# Epsilon -- 2011

- Epsilon, an email service provider for companies, reported a breach that affected approximately 75 client companies.
- Email addresses and customer names were affected.
- Epsilon has not disclosed the names of the companies affected or the total number of names stolen. However, millions of customers received notices from a growing list of companies, **making this the largest security breach ever**.
- Conservative estimates place the number of customer email addresses breached at 50 to 60 million. The number of customer emails exposed may have reached 250 million.
- Compromised email addresses and names may seem innocuous to some, but victims may fall prey to *spear phishing*.

Source: Privacy Rights Clearinghouse, December 16, 2011

# Epsilon -- 2011

- Spear phishing occurs when a criminal sends an email that sounds and looks like it's from a company the recipient has an account with because it addresses him or her by name.
- A spear-phishing message might say, "Hello Mr. Berthing, Because of the recent hacking incident affecting some Acme customers, we are asking you to visit this website [URL provided] and update your security settings."
- The email tries to convince trusting readers to "bite" on the bait and go to that website, and then divulge other information like Social Security numbers and credit card numbers. The result could be as serious as identity theft.
- The Epsilon breach is also significant because it highlights the risk of cloud-based computing systems and the need for greater cloud security measures.

Source: Privacy Rights Clearinghouse, December 16, 2011

# Sutter Physicians Services (SPS) and Sutter Medical Foundation (SMF) 2011

- A company-issued desktop computer was stolen from SMF's administrative offices in California
- Data was password protected, it was not encrypted.
- Approximately 3.3 million patients whose health care provider is supported by SPS had their names, addresses, dates of birth, phone numbers, email addresses, medical record numbers and health insurance plan name exposed.
- Additional 934,000 SMF patients had dates of services and description of medical diagnoses and/or procedures used for business operations

Source: Privacy Rights Clearinghouse, December 16, 2011

# Sutter Physicians Services (SPS) and Sutter Medical Foundation (SMF) 2011

- At least two lawsuits have been filed against Sutter Health. One class-action suit alleges that Sutter Health was negligent in safeguarding its computers and data, and then did not notify the millions of patients whose data went missing within the time required by state law.
- The security lapse occurred on two levels: both the data itself (being unencrypted) and the physical location (stored in an unsecure location).
- Although no Social Security numbers or financial information were apparently exposed, all the data elements needed for medical identity theft were included in the stolen records.

Source: Privacy Rights Clearinghouse, December 16, 2011

# Heartland Payment Systems -- 2009

- Largest credit card crime of all time
- Hackers broken into computers
  - Process about 100 million transactions each month for 175,000 merchants
- Uncovered in January, after Visa and MasterCard notified about suspicious transactions
- August 2009, three men were indicted by a grand jury on charges related to masterminding a scheme to steal more than 130 million credit and debit card numbers and personally identifying information from Heartland, 7-Eleven Inc. and other companies
- Heartland agreed to pay MasterCard issuers $41.4 million to settle claims over the data breach, according to The Associated Press.

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# TJX Companies -- 2007

- One of the first to show how vulnerable retailers were
- December 2006 TJX alerted law enforcement that cybercriminals had stolen more than 45 million customer records in 2003 and 2004.
- In January 2007 it went public with the news.
- Within eight months spent more than $20 million investigating the incident, notifying customers and hiring lawyers to deal with the dozens of associated lawsuits.
- The hack alerted the industry to the threat of cybercriminals and pushed lawmakers to fast-track data security legislation

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# U.S. Department of Veterans Affairs-2009

- Personal information for as many as 76 million veterans might have been compromised when a defective hard drive was sent for repair and recycling without first having the data on it erased
- In October 2009, the National Archives and Records Administration investigated the Veterans Affairs agency for the potential data breach
- The hard drive was used for the system veterans used to request health records and discharge papers, and included millions of Social Security numbers

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# Card Systems -- 2005

- June 2005, news broke that a security breach at CardSystems, an Atlanta-based third-party processor of payment card transactions exposed more than 40 million card accounts to potential fraud.
- Of those, 68,000 Mastercard accounts, 100,000 Visa accounts and 30,000 accounts from other brands are known to have been used by hackers, according to the Privacy Rights Clearinghouse.

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# Veterans Laptop With Personal Data Stolen

- In May 2006, U.S. Veterans Affairs officials disclosed that a laptop containing personal information for millions of veterans had been stolen in a burglary from the home of an agency employee in Maryland.
- The agency estimated that about 17.5 million veterans were at risk and reportedly offered to cover the cost of monitoring their credit for one year, to the tune of $160.5 million.
- Fortunately, about a month later, the FBI announced it had recovered the laptop and the personal information had not been compromised.

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# Bank of New York Mellon -- 2008

- The personal information for more than 12.5 million people was potentially compromised when the Bank of New York Mellon lost of box of computer data tapes with information such as Social Security numbers, names, addresses and possibly bank account numbers.
- The six to 10 tapes were lost en route to a storage facility
- February 2008, Connecticut officials disclosed the breach, saying more than 4.5 million people were affected.
- August 2008, the number was raised to 12.5 million.
- A year later, the bank agreed to pay Connecticut $150,000 as part of a settlement and provide credit monitoring and fraud alerts for the affected people for 36 months.
- It also agreed to reimburse customers for funds stolen as a result of the breach

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# Certegy -- 2007

- In 2007, Certegy Check Services, a financial services firm, disclosed that an employee stole customer records that included credit card, bank account and other personal information
- Though the company first estimated that the breach affected about 2.3 million people, later it upped the number to 8.5 million.
- The employee responsible for the breach pleaded guilty to fraud and conspiracy charges and was sentenced to time in jail as well as a multi-million dollar fine.
- In April 2010, Certegy agreed to donate $125,000 to the Florida Attorney General's Seniors vs. Crime Program and $850,000 for the state's investigative costs and fees related to the case.

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# TD Ameritrade -- 2007

- TD Ameritrade an online trading and investing company, revealed in 2007 that information for more than 6.3 million customers was stolen when one of its databases was hacked.
- According to Privacy Rights, the company said at the time that names, e-mail addresses, phone numbers and addresses were lifted in the breach, which meant that customers received spam as a result.

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# CheckFree -- 2008

- In 2008, CheckFree Corp., an online bill paying company, reported that hackers hijacked several of the company's Internet domain names and redirected customers to a Web site hosted in Ukraine that tried to install malware on peoples' computers.
- At the time, the company estimated that about 160,000 people were exposed to the malicious site. But because hackers compromised the company's domain name, as many as 5 million people might have been affected, according to the Privacy Rights Clearinghouse.

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# Hannaford Bros. Chain -- 2009

- Hannaford Bros. Co., a supermarket chain, disclosed in 2008 that a security breach affected hundreds of its stores in the Northeast and Florida.
- The company reported about 1,800 cases of alleged fraud related to the breach.
- According to Privacy Rights, as many as 4.2 million people could have been compromised by the intrusion, which resulted in stolen credit and debit card numbers.

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011

# Certegy -- 2007

- In 2007, Certegy Check Services, a financial services firm, disclosed that an employee stole customer records that included credit card, bank account and other personal information
- Though the company first estimated that the breach affected about 2.3 million people, later it upped the number to 8.5 million.
- The employee responsible for the breach pleaded guilty to fraud and conspiracy charges and was sentenced to time in jail as well as a multi-million dollar fine.
- In April 2010, Certegy agreed to donate $125,000 to the Florida Attorney General's Seniors vs. Crime Program and $850,000 for the state's investigative costs and fees related to the case.

Source: Privacy Rights Clearinghouse/ ABC News June 14, 2011